

Universal Strongly Secure Network Coding with Dependent and Non-Uniform Messages

Ryutaro Matsumoto, *Member, IEEE*, and Masahito Hayashi, *Member, IEEE*

Abstract—We consider the random linear precoder at the source node as a secure network coding. We prove that it is strongly secure in the sense of Harada and Yamamoto [22] and universal secure in the sense of Silva and Kschischang [31], [32], while allowing arbitrary small but nonzero mutual information to the eavesdropper. Our security proof allows statistically dependent and non-uniform multiple secret messages, while all previous constructions of weakly or strongly secure network coding assumed independent and uniform messages, which are difficult to be ensured in practice.

Index Terms—information theoretic security, network coding, secure multiplex coding, strongly secure network coding

I. INTRODUCTION

Network coding [1] attracts much attention recently because it can offer improvements in several metrics, such as throughput and energy consumption, see [19], [20]. On the other hand, the information theoretic security [6], [28] also attracts much attention because it offers security that does not depend on a conjectured difficulty of some computational problem.

A juncture of the network coding and the information theoretic security is the secure network coding [9], [12], which prevents an eavesdropper, called Eve, from knowing the message from the legitimate sender, called Alice, to the multiple legitimate receivers by eavesdropping intermediate links up to a specified number in a network. It can be seen [15], [16] as a network coding counterpart of the traditional wiretap channel coding problem considered by Wyner [34] and subsequently others [28]. In both secure network coding and coding for wiretap channels, the secrecy is realized by including random bits into the transmitted signal by Alice so that the secret message becomes ambiguous to Eve. The inclusion of random bits, of course, decreases the information rate. In order to get rid of the decrease in the information rate, Yamamoto et al. [25] proposed the secure multiplex coding for

wiretap channels, in which there is no loss of information rate. The idea of Yamamoto et al. is as follows: Suppose that Alice has T statistically independent messages S_1, \dots, S_T . Then $S_1, \dots, S_{i-1}, S_{i+1}, \dots, S_T$ serve as the random bits making S_i ambiguous to Eve, for each i .

Independently and simultaneously, Bhattad and Narayanan [3] proposed the weakly secure network coding based on the same idea as [25], whose goal is also to get rid of the loss of information rate in the secure network coding. Their method [3] ensures that the mutual information between S_i and Eve's information is zero for each i . Recall that Eve's knowledge on secret information S_i is usually measured by the mutual information in the information theoretic security [6], [28]. As drawbacks, the construction depends on the network topology and coding at intermediate nodes, and the computational complexity of code construction is large.

Harada and Yamamoto [22] defined a stronger security requirement on the weakly secure network coding, which will be reviewed later, and called it as the strongly secure network coding. Then they showed its construction procedure. As [3], the construction depends on the network topology and coding at intermediate nodes, and the computational complexity of code construction is large.

In order to remove these drawbacks, Silva and Kschischang [31] proposed the universal weakly secure network coding, in which they showed an efficient code construction that can support up to two \mathbf{F}_q -symbols in each S_i and is independent of the network topology and coding at intermediate nodes, where \mathbf{F}_q denotes the finite field with q elements throughout this paper. The independence of coding at the source node from network topology and coding at intermediate nodes is termed universal by Silva and Kschischang in [31], [32]. They [31] also showed the existence of universal weakly secure network coding with more than two \mathbf{F}_q -symbols in S_i , but have not shown an explicit construction.

Cai [7] removed most of drawbacks mentioned earlier. Cai proved that random linear network coding [24] gives the strongly secure network coding in the sense of [22] with arbitrarily high probability with sufficiently large finite fields. However, he did not provide evaluation of the required field size, and it seems huge. Moreover, for some applications (e.g. [10], [36]) we want to choose coding at intermediate nodes in non-random fashion.

There exists a common difficulty in all the previous constructions reviewed above. In practice, we are not sure if the multiple messages are uniform and statistically independent.

This research was partially supported by the MEXT Grant-in-Aid for Young Scientists (A) No. 20686026, (B) No. 22760267, Grant-in-Aid for Scientific Research (A) No. 23246071, and the Villum Foundation through their VELUX Visiting Professor Programme 2011–2012. The Center for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme. This paper was presented in part at 2011 IEEE International Symposium on Network Coding, Beijing, China, July 2011 [30], and in part at 2011 IEEE International Symposium on Information Theory, Saint Petersburg, Russia, August 2011 [29].

R. Matsumoto is with Department of Communications and Integrated Systems, Tokyo Institute of Technology, 152-8550 Japan (email: ryutaro@it.ss.titech.ac.jp, TEL: +81 3 5734 3864, FAX: +81 3 5734 2905).

M. Hayashi is with Graduate School of Mathematics, Nagoya University, 464-8602 Japan, and Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117542 (email: masahito@math.nagoya-u.ac.jp).

However, all the previous studies¹ assumed the uniformity and the independence, and without both of them their security proofs do not seem to hold. It is important to provide a security proof for weakly and strongly secure network coding without uniformity or independence assumption. On the other hand, non-uniformity of secret messages has been considered in the ordinary secure network coding [11], [37] (see also the survey [8]). In [8], [11], [37], the randomness to hide a secret message was assumed to be statistically independent of the secret message, while our present study allows it to be statistically dependent.

We shall analyze the security of a slightly modified construction of the random linear precoder originally proposed in [9]. Our modified construction is strongly secure in the sense of [22] and universal secure in the sense of [31], [32]. Uniformity and the independence assumptions are required in previous works to guarantee security. This paper relaxed the assumptions and aims to determine the amount of information leakage if the two conditions are not satisfied. The optimality of our modified construction is verified under the uniformity and independence assumption at the end of Remark 8.

However, we relax an aspect of the security requirements traditionally used in the secure network coding. In previous proposals of secure network coding [3], [9], [22], [31], [32] it is required that the mutual information to the eavesdropper is exactly zero. We relax this requirement by regarding sufficiently small mutual information to be acceptable. This relaxation is similar to requiring the decoding error probability to be sufficiently small instead of strictly zero. Also observe that our relaxed criterion is much stronger than one commonly used in the information theoretic security [28]. Our modified construction can realize arbitrary small mutual information if coding over sufficiently many symbols in single packet is allowed. We stress that the problem of secure network coding is a generalization of the secret sharing [4], [33] and the former problem cannot be solved as the latter, as clearly observed in, e.g. [8], [12]. Because we have to show the security under much more eavesdropper's choices in secure network coding than that in secret sharing scheme, as is explained at the end of Subsection III-C.

This paper is organized as follows: Section II reviews related results used in this paper. Section III introduces the strengthened version of the privacy amplification theorem and the proposed scheme for secure network coding. Section IV concludes the paper.

Part of this paper was reported as earlier proceedings papers [29], [30]. We substantially rewrote our security proof in [30] so that we can analyze the security with dependent and non-uniform multiple secret messages, which was not done in [30]. We borrowed ideas from [29, Section IV] and extended them in Appendix B so that we can prove Lemma 5.

¹Cai [7] considered arbitrary probability distribution in [7, Theorem 3.2] but assumed uniformity and independence for his study of the strongly secure network coding in [7, Section IV].

II. PRELIMINARY

A. Model of network and network coding and two-universal hash functions

As in [3], [9], [12], [22], [31], [32] we consider the single source multicast, and assume the linear network coding [26], [27]. The source node is assumed to have at least n outgoing links. For $i = 1, \dots, n$, the source node generates a packet P_i consisting of m symbols in \mathbf{F}_q , and transmits an \mathbf{F}_q -linear combination of P_1, \dots, P_n to each outgoing link, as explained in [18, Section 2.1]. At an intermediate node, only packets generated at the same time by the source node are linearly combined, as explained in [18, Section 2.5]. The linear combination coefficients at each node are fixed so that all the legitimate receivers can decode n packets P_1, \dots, P_n from the source node.

If the random linear network coding [24] is employed, we have to also include so-called encoding vectors in each packet P_i [18, Section 2.2]. We ignore those encoding vectors because they do not carry secret information.

Hereafter, we shall only consider the eavesdropper Eve and forget about the multiple legitimate receivers. The n packets P_1, \dots, P_n carry in total mn symbols in \mathbf{F}_q . We shall propose a method encoding secret information into mn symbols by the source node. The mn symbols obtained by the proposed method are distributed to packets P_1, \dots, P_n .

Eve can eavesdrop μ links. We assume $\mu \leq n$ throughout this paper. The total number of eavesdropped symbols is therefore $m\mu$. The set of μ eavesdropped links is assumed to be fixed during packets P_1, \dots, P_n are traveling on the network, as assumed in [31], [32]. The situation considered here also includes the conventional store-and-forward network as a special case.

We shall use a family of two-universal hash functions [13] for the privacy amplification theorem introduced later.

Definition 1: Let \mathcal{F} be a set of functions from a finite set \mathcal{S}_1 to another finite set \mathcal{S}_2 , and F a random variable on \mathcal{F} . If for any $x_1 \neq x_2 \in \mathcal{S}_1$ we have

$$\Pr[F(x_1) = F(x_2)] \leq \frac{1}{|\mathcal{S}_2|}, \quad (1)$$

then \mathcal{F} with the probability distribution of F is said to be a *family of two-universal hash functions*.

B. Security definitions

Definition 2 (Strongly secure network coding): [22] Let $m = 1$, and $S_1, \dots, S_T \in \mathbf{F}_q$ be messages with $T \leq n$. We denote by $S_{T+1}, \dots, S_n \in \mathbf{F}_q$ randomness not intended as messages. A network coding is said to be η -strongly secure if the following relation holds for any $0 \leq \mu \leq n$. When Eve's observation Z is obtained by eavesdropping μ links, any $I \subset \{1, \dots, T\}$ with $\mu - \eta \leq T - |I|$ satisfies

$$I(S_I; Z) = 0,$$

where $S_I = [S_i : i \in I]$ and $I(S_I; Z)$ denotes their mutual information as defined in [14].

The parameter η is equivalent to k in [22]. Harada and Yamamoto [22] showed a procedure to construct $(n - T)$ -strongly secure network coding under the uniformity and independence assumption on the messages S_1, \dots, S_n .

We want to consider the universal security studied in [31], [32], and also want to use multiple symbols in a single packet P_i , that is, $m > 1$. So we introduce our version of universal strong security, by following the approach initiated by Silva and Kschischang [31], [32].

Definition 3: Assume that we are given a linear network coding for single source multicast. Assume also that linear coding at intermediate nodes and the set of μ eavesdropped links are fixed when packets P_1, \dots, P_n travel from the source node to all the legitimate receivers. Suppose that we have $T+1$ messages S_1, \dots, S_{T+1} and $S_i \in \mathbb{F}_q^{k_i}$. S_{T+1} denotes randomness not intended as a message. We assume $\sum_{i=1}^{T+1} k_i = mn$. A linear transformation of S_1, \dots, S_{T+1} at the source node is said to be a universal η -strongly secure network coding if the following relation holds for all linear coding at intermediate nodes and for any $0 \leq \mu \leq n$. When Eve's observation Z corresponds to μ eavesdropped links, any subset $\mathcal{I} \subset \{1, \dots, T\}$ with $m(\mu - \eta) < \sum_{1 \leq i \leq T+1, i \notin \mathcal{I}} k_i$ satisfies

$$I(S_{\mathcal{I}}; Z) = 0, \quad (2)$$

where $S_{\mathcal{I}} = [S_i : i \in \mathcal{I}]$.

III. UNIVERSAL STRONGLY SECURE NETWORK CODING

A. Strengthened privacy amplification theorem

In order to evaluate the mutual information to Eve when the sum rate of multiple secret information is large, we need to strengthen the privacy amplification theorem originally appeared in [2], [23] as follows. The following proposition is a slightly enhanced version of [30, Theorem 2].

Proposition 4: Let A_1 and A_2 be discrete random variables on finite sets \mathcal{A}_1 and \mathcal{A}_2 , respectively, and \mathcal{F} a family of functions from \mathcal{A}_1 to \mathcal{A}_3 . Let F be a random variable on \mathcal{F} . Assume that A_1 and F are conditionally independent given A_2 , and that for any fixed realization a_2 of A_2 , the conditional probability distribution of F given a_2 satisfies the condition for a family of two-universal hash functions. Then we have

$$\mathbf{E}_f[\exp(\rho I(F(A_1); A_2 | F = f))] \leq 1 + |\mathcal{A}_3|^\rho \mathbf{E}[P_{A_1|A_2}(A_1 | A_2)^\rho] \quad (3)$$

for all $0 \leq \rho \leq 1$, where $\mathbf{E}_f[\cdot]$ denotes the expectation of \cdot with f being the random variable. We use the natural logarithm for all the logarithms in this paper, which include ones implicitly appearing in entropy and mutual information. Otherwise we have to adjust the above inequality.

Proof: Proof is given in Appendix A. ■

In our analysis of the security, we shall use Proposition 4 with A_1 being the whole secret message, A_2 being part of the secret message whose secrecy we analyze, and $F(A_1)$ being Eve's observation.

B. Description of the proposed scheme and analysis with randomized coding

The purpose of this section is to provide a universal $(k_{T+1}/m - \delta_\rho)$ -strongly secure network coding in a slightly modified sense of Definition 3, where δ_ρ is a parameter measuring

conditional non-uniformity to be defined in Eq. (12). The modified sense means that the zero mutual information in Eq. (2) is relaxed to the requirement that it can be made arbitrarily small. For this purpose, in this subsection, we treat the coding scheme with randomized coding. We assume that we have T secret messages, which can be dependent or non-uniform, and that the i -th secret message is given as a random variable S_i whose realization is a row vector in $\mathbb{F}_q^{k_i}$. We shall provide upper bounds on the information leaked to Eve for all choices of values of k_i . We shall also use a supplementary random message S_{T+1} taking values in $\mathbb{F}_q^{k_{T+1}}$ when the randomness in the encoder is insufficient to make S_i secret from Eve. By S we denote the entire collection (S_1, \dots, S_{T+1}) of messages. We assume $mn = k_1 + \dots + k_{T+1}$.

Let \mathcal{L} be the set of all bijective \mathbb{F}_q -linear maps from $\prod_{i=1}^{T+1} \mathbb{F}_q^{k_i}$ to itself, and L the uniform random variable on \mathcal{L} statistically independent of $S = (S_1, \dots, S_{T+1})$, and arbitrary fix nonempty $\mathcal{I} \subseteq \{1, \dots, T\}$. The source node store LS^t into packets P_1, \dots, P_n defined in Section II-A and send them via its n outgoing links, where t denotes the transpose of a vector. Our modified construction just attaches a bijective linear function to an existing network coding. Note that attaching a random linear function was first proposed in [9] for the secure network coding. This coding scheme is illustrated in Fig. 1.

The legitimate sender and all the legitimate receivers agree on the choice of L . The eavesdropper Eve may also know their choice of L . Choice of L is part of protocol specification, the chosen L is repeatedly used, and agreement on its choice among legitimate sender and receivers is not counted as consumption of the network bandwidth. A legitimate receiver can recover S_1, \dots, S_T, S_{T+1} by multiplying L^{-1} to his/her received information. By the assumption on Eve, her information can be expressed as BLS^t by using an $m\mu \times mn$ matrix B over \mathbb{F}_q as in [31], [32].

For the nonempty $\mathcal{I} \subseteq \{1, \dots, T\}$, denote the collection of random variables $[S_i : i \in \mathcal{I}]$ by $S_{\mathcal{I}}$, denote $[S_i : i \in \{1, \dots, T+1\} \setminus \mathcal{I}]$ by $S_{\bar{\mathcal{I}}}$, and let $k_{\mathcal{I}} = \sum_{i \in \mathcal{I}} k_i$.

For a fixed realization ℓ of L , the information gained by Eve is measured by the mutual information $I(S_{\mathcal{I}}; BLS^t | L = \ell)$ as a common practice in the information theoretic security [6], [28]. Since its average $\mathbf{E}_\ell[I(S_{\mathcal{I}}; BLS^t | L = \ell)]$ is the conditional mutual information $I(S_{\mathcal{I}}; BLS^t | L)$ [14], we will upper bound $I(S_{\mathcal{I}}; BLS^t | L)$. After upper bounding the average $I(S_{\mathcal{I}}; BLS^t | L)$ in Eq. (5), we can ensure that for most choices of ℓ and all possible B , $I(S_{\mathcal{I}}; BLS^t | L = \ell)$ is small, as done in Eq. (11).

In order to use Proposition 4, we introduce a lemma.

Lemma 5: For fixed B , the family of mapping $S \mapsto BLS^t$ is a family of two-universal hash functions to the $\text{rank}(B)$ -dimensional \mathbb{F}_q -linear space.

Proof: See Appendix B. ■

We can upper bound $I(S_{\mathcal{I}}; BLS^t | L)$ as follows, by applying Proposition 4 with $A_1 = S$, $A_2 = S_{\mathcal{I}}$, and $F(A_1) = BLS^t$. Observe that the assumption in Proposition 4 holds because $S_{\mathcal{I}}$ is part of S and L is independent of S .

$$\begin{aligned} & \mathbf{E}_\ell[\exp(\rho I(S_{\mathcal{I}}; BLS^t | L = \ell))] \\ & \leq 1 + q^{m\rho \times \text{rank}(B)} \mathbf{E}[P_{S|S_{\mathcal{I}}}(S | S_{\mathcal{I}})^\rho] \end{aligned}$$

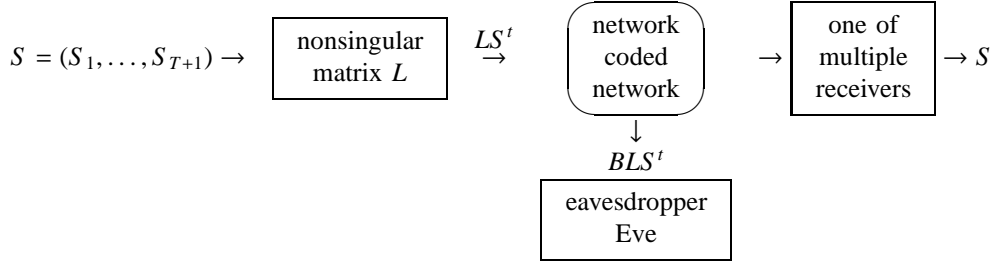


Fig. 1. Proposed coding scheme for the universal strongly secure network coding

$$\begin{aligned}
 &= 1 + q^{m\rho \times \text{rank}(B)} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho] \\
 &\leq 1 + q^{m\rho\mu} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho].
 \end{aligned} \quad (4)$$

From Eq. (4) we have

$$\begin{aligned}
 &\rho I(S_I; BLS^t|L) \\
 &= \ln \exp(\rho I(S_I; BLS^t|L)) \\
 &\leq \ln \mathbf{E}_\ell[\exp(\rho I(S_I; BLS^t|L = \ell))] \\
 &\leq \ln(1 + q^{m\rho\mu} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho]) \\
 &\leq q^{m\rho\mu} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho].
 \end{aligned} \quad (5)$$

Fix a real number $C_1 > 1$. Equation (5) and the Markov inequality yield that

$$\Pr[\ell \in \mathcal{L}_{I,1}] < 1/C_1$$

for any single nonempty $I \subseteq \{1, \dots, T\}$, where $\mathcal{L}_{I,1} := \{\ell \mid I(S_I; BLS^t|L = \ell) > C_1 \mathbf{E}_\ell[I(S_I; BLS^t|L = \ell)]\}$. Thus,

$$\Pr[\ell \in \cup_{I: I \neq \emptyset} \mathcal{L}_{I,1}] < (2^T - 1)/C_1.$$

This means that there is at least a probability of $1 - (2^T - 1)/C_1$ such that a realization ℓ of L satisfies

$$\begin{aligned}
 &I(S_I; BLS^t|L = \ell) \\
 &\leq C_1 \mathbf{E}_\ell[I(S_I; BLS^t|L = \ell)] \\
 &\leq C_1 q^{m\rho\mu} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho] / \rho
 \end{aligned} \quad (6)$$

for all the $(2^T - 1)$ nonempty subsets I of $\{1, \dots, T\}$. Defining another subset $\mathcal{L}_{I,2} := \{\ell \mid \exp(\rho I(S_I; BLS^t|L = \ell)) > C_1 \mathbf{E}_\ell[\exp(\rho I(S_I; BLS^t|L = \ell))]\}$, by Eq. (4) and the Markov inequality we obtain

$$\Pr[\ell \in \cup_{I: I \neq \emptyset} (\mathcal{L}_{I,1} \cup \mathcal{L}_{I,2})] < 2(2^T - 1)/C_1.$$

Therefore, a realization ℓ of L satisfies both Eq. (6) and

$$\exp(\rho I(S_I; BLS^t|L = \ell)) \leq C_1(1 + q^{m\rho\mu} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho]). \quad (7)$$

with probability at least $1 - 2 \times (2^T - 1)/C_1$.

Equation (7) implies

$$\begin{aligned}
 &\frac{I(S_I; BLS^t|L = \ell)}{m} \\
 &= \frac{1}{m} \ln \exp I(S_I; BLS^t|L = \ell) \\
 &\leq \frac{\ln C_1}{m\rho} + \frac{1}{m\rho} \ln(1 + q^{m\rho\mu} \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho]) \quad (\text{by Eq. (7)}) \\
 &\leq \frac{\ln C_1}{m\rho} + \left| \mu \ln q + \frac{1 + \ln \mathbf{E}[P_{S_{\bar{T}}|S_I}(S_{\bar{T}}|S_I)^\rho]}{m\rho} \right|^+,
 \end{aligned} \quad (8)$$

where in Eq. (8) we used $\ln(1 + \exp(x)) \leq |1 + x|^+ = \max\{0, 1 + x\}$.

Summarizing the preceding discussion, we have the following theorem.

Theorem 6: Recall that the eavesdropping $m\mu \times mn$ matrix B is fixed, that L is the uniform random variable on \mathcal{L} statistically independent of $S = (S_1, \dots, S_{T+1})$, and that a real number $C_1 > 1$ is arbitrarily fixed. There is at least a probability of $1 - 2 \times (2^T - 1)/C_1$ such that information leakage $I(S_I; BLS^t|L = \ell)$ to Eve with the chosen realization ℓ of L satisfies both inequalities (6) and (8) simultaneously.

C. Evaluation of the number of different kinds of eavesdropping

In the following, we considered the case when the matrix B corresponds to μ eavesdropped links. Such a case can be mathematically formulated as follows. Let $x_{i,j} \in \mathbb{F}_q$ be the j -th symbol in the i -th packet P_i defined in Section II-A. Then there exists a $\mu \times n$ matrix $B_{\mu \times n}$ such that what are observed by Eve at the j -th symbols in her eavesdropped μ packets is expressed as $B_{\mu \times n}(x_{1,j}, \dots, x_{n,j})^t$ for $j = 1, \dots, m$. Without loss of generality we may assume $\text{rank}(B_{\mu \times n}) = \mu$ because if $\text{rank}(B_{\mu \times n}) = \mu' < \mu$ then such a case can be regarded as only μ' links being eavesdropped. Then, the $m\mu \times mn$ matrix² B is completely determined by $B_{\mu \times n}$.

In order to show the universal security in Definition 3, we need to ensure that the mutual information is small for any B and any $0 \leq \mu \leq n$. For this purpose, we need to count the number of different kinds of eavesdropping, which is much larger than that in the secret sharing scheme [4], [33].

We consider the set $\mathcal{B}(\mu)$ of all possible $m\mu \times mn$ matrices B that characterize Eve's eavesdropping with the above restriction. Then, we define an equivalence relation \sim on $\mathcal{B}(\mu)$ as $B_1 \sim B_2$ for $B_1, B_2 \in \mathcal{B}(\mu)$ if there exists an invertible function f such that $f(B_1 LS^t) = B_2 LS^t$ for all L and S^t . That is, $B_1 \sim B_2$ if and only if the kernel of B_1 is the same as that of B_2 . Since B_1 and B_2 are determined by $\mu \times n$ matrixes, the space $\mathcal{B}(\mu)/\sim$ is the set of the $(n - \mu)$ -dimensional subspaces in \mathbb{F}_q^n . The space is called Grassmannian and the number is evaluated in the following way [17]

$$|\mathcal{B}(\mu)/\sim| = \prod_{i=0}^{\mu-1} \frac{q^n - q^i}{q^\mu - q^i} \leq \prod_{i=0}^{\mu-1} \frac{q^n - q^{\mu-1}}{q^\mu - q^{\mu-1}} = \prod_{i=0}^{\mu-1} \frac{q^{n-\mu+1} - 1}{q - 1}$$

²Mathematically, the $m\mu \times mn$ matrix B is written as $B_{\mu \times n} \otimes I_{m \times mn}$.

$$\leq \prod_{i=0}^{\mu-1} q^{n-\mu+1} = q^{\mu(n-\mu+1)} \leq q^{\frac{(n+1)^2}{4}} \quad (9)$$

because $(x-z)/(y-z)$ is monotone increasing concerning z when $x > y > z > 0$. The final inequality follows from the inequality $\sqrt{\mu(n-\mu+1)} \leq \frac{\mu+n-\mu+1}{2} = \frac{n+1}{2}$. Hence, the total number of equivalence classes excluding $B(0)$ is upper bounded as

$$\sum_{\mu=1}^n |\mathcal{B}(\mu)| \sim |\leq nq^{\frac{(n+1)^2}{4}}. \quad (10)$$

Conversely, in order to compare the number of kinds of information leakage with the secret sharing scheme, we check the tightness of evaluation (9), i.e., we show the opposite inequality. Since $(x-z)/(y-z) > x/y$ holds for $x > y > z > 0$,

$$|\mathcal{B}(\mu)| \sim |\leq \prod_{i=0}^{\mu-1} \frac{q^n - q^i}{q^\mu - q^i} \geq \prod_{i=0}^{\mu-1} \frac{q^n}{q^\mu} = q^{\mu(n-\mu)}.$$

That is, when μ is fixed, the number of possible kinds of information leakage is greater than $q^{\mu(n-\mu)}$ in the network coding scheme. On the other hand, in the secret sharing scheme, the possible information leakage is given as an observation of μ shares among n shares, the number is $\binom{n}{\mu}$, which grows up only polynomially of n with a fixed μ . Therefore, the universal code in the network coding scheme has to satisfy the universality under much more choices of eavesdropper than that in the ramp secret sharing scheme [5], [35].

D. Universally strongly secure networking code

Next, using the above discussion, we show the existence of universally strongly secure networking code. Due to (10), the probability of L satisfying Eqs. (6) and (8) simultaneously for all possible B is at least

$$1 - 2 \times (2^T - 1) \times nq^{\frac{(n+1)^2}{4}} / C_1. \quad (11)$$

Recall that chosen L is part of protocol specification and repeatedly used. Because Eqs. (6), (8) and (11) are independent of realization of the random variable S representing secret information, Eqs. (6) and (8) are satisfied in every repeated use of L with probability at least Eq. (11).

The upper bound (6) can go to either zero or ∞ as $m \rightarrow \infty$. When the upper bound (6) goes to ∞ , the information leakage to Eve grows linearly with m and its growth rate with m will be analyzed by Eq. (8). Firstly, we need to clarify under what condition Eq. (6) converges to zero as $m \rightarrow \infty$. To do so, we shall introduce a version of conditional Rényi entropy introduced in [23]. There seems to be no standard definition for the conditional Rényi entropy, for example, definitions in [2] and [21] disagree and our definition in [23] is different from [2], [21]. For discrete random variables X , Y , define conditional Rényi entropy of order $1 + \rho$ as

$$H_{1+\rho}(X|Y) = -\frac{\log_q \mathbf{E}[P_{X|Y}(X|Y)^\rho]}{\rho}.$$

For $\rho = 0$, we define $H_1(X|Y)$ as $\lim_{\rho \rightarrow 0} H_{1+\rho}(X|Y)$. By using l'Hôpital's rule we see that $H_1(X|Y)$ is equal to the conditional Shannon entropy. Observe also that $H_{1+\rho}(X|Y) = \log_q |\mathcal{X}|$ if X

is conditionally uniform given Y , where \mathcal{X} denotes the alphabet of X .

In order to clarify under what condition Eq. (6) converges to zero, we need to assume some knowledge on $P_{S_{\mathcal{I}}|S_{\mathcal{I}}}(S_{\mathcal{I}}|S_{\mathcal{I}})$. We consider the situation in which each message S_i originates from a different organization and it is compressed before network coded. Under such situation, we assume that $S_{\mathcal{I}}$ is nearly conditionally uniform given $S_{\mathcal{I}}$. Let δ_ρ be a nonnegative constant such that

$$n - \frac{k_{\mathcal{I}}}{m} - \frac{H_{1+\rho}(S_{\mathcal{I}}|S_{\mathcal{I}})}{m \ln q} \leq \delta_\rho \quad (12)$$

for some $0 < \rho \leq 1$, for all \mathcal{I} , and for sufficiently large m . Observe that if all messages S_i 's are uniform and independent then $\delta_\rho = 0$. The parameter δ_ρ captures the deviation from the uniform and independent situation in terms of conditional Rényi entropy per the number m of symbols in single packet. By taking the natural logarithm of Eq. (6), we see

$$\begin{aligned} & \ln [\text{RHS of Eq. (6)}] \\ &= \ln \frac{C_1}{\rho} + m\rho(\mu \ln q + \frac{\ln \mathbf{E}[P_{S_{\mathcal{I}}|S_{\mathcal{I}}}(S_{\mathcal{I}}|S_{\mathcal{I}})^\rho]}{m\rho}) \\ &= \ln \frac{C_1}{\rho} + m\rho(\mu - \frac{H_{1+\rho}(S_{\mathcal{I}}|S_{\mathcal{I}})}{m}) \ln q. \end{aligned} \quad (13)$$

When

$$\mu < (n - \frac{k_{\mathcal{I}}}{m}) - \delta_\rho \text{ i.e. } \frac{k_{\mathcal{I}}}{m} < n - \mu - \delta_\rho, \quad (14)$$

(*) in Eq. (13) becomes negative by Eq. (12). Under such condition Eq. (13) converges to $-\infty$ as $m \rightarrow \infty$, which means that the upper bound Eq. (6) can be made arbitrary small by letting m be large.

Secondly, we shall analyze how much information Eve can gain when Eq. (14) does not hold. In such case we use the other upper bound Eq. (8). We can rewrite Eq. (8) as

$$\begin{aligned} & \text{RHS of Eq. (8)} \\ &= \frac{1 + \ln C_1}{m\rho} + \mu \ln q - \frac{H_{1+\rho}(S_{\mathcal{I}}|S_{\mathcal{I}})}{m} \\ &\leq \frac{1 + \ln C_1}{m\rho} + (\mu - (n - \frac{k_{\mathcal{I}}}{m} - \delta_\rho)) \ln q \text{ (by Eq. (12))}. \end{aligned}$$

We see that we can make the upper bound Eq. (8) on $\frac{I(S_{\mathcal{I}}; BLS^{\mathcal{I}}|L=\ell)}{m}$ arbitrary close to

$$(\mu + \delta_\rho - (n - \frac{k_{\mathcal{I}}}{m})) \ln q \quad (15)$$

by letting m be large.

By the above modified construction and evaluation of mutual information, we provide a universal $(k_{T+1}/m - \delta_\rho)$ -strongly secure network coding in the sense of Definition 3 with the zero mutual information requirement in Eq. (2) replaced by arbitrary small one (see also Remark 8).

Remark 7: The meaning of C_1 is as follows: At Eqs. (4) and (5), there might not exist a realization ℓ of L that satisfies Eqs. (4) and (5) for all subsets \mathcal{I} of $\{1, \dots, T\}$ simultaneously. By sacrificing the tightness of the upper bounds, we ensure the existence of ℓ satisfying Eqs. (6) and (7) for all \mathcal{I} .

Remark 8: Under the assumption that all messages S_1, \dots, S_{T+1} are uniform and independent, the mutual information can be made exactly zero for every eavesdropping matrix B . The reason is as follows: For fixed B and $L = \ell$, we have

$$I(S_I; BLS^t | L = \ell) = H(S_I | L = \ell) - H(S_I | BLS^t, L = \ell). \quad (16)$$

The first term $H(S_I | L = \ell)$ is an integer multiple of $\ln q$ since S_I is assumed to have the uniform distribution. Let α_I be the projection from $\prod_{i=1}^{T+1} \mathbf{F}_q^{k_i}$ to $\prod_{i \in I} \mathbf{F}_q^{k_i}$ for $\emptyset \neq I \subseteq \{1, \dots, T\}$. For fixed B and ℓ , and a given realization z of $B\ell S^t$, the set of solutions s such that $z = B\ell s$ is written as $\ker(B\ell) +$ some vector v . This means that the set of possible candidates of S_I given realization z of $B\ell S^t$ is written as $\alpha_I(\ker(B\ell)) + \alpha_I(v)$, and S_I given realization z is uniformly distributed on $\alpha_I(\ker(B\ell)) + \alpha_I(v)$. Since the cardinality of $\alpha_I(\ker(B\ell)) + \alpha_I(v)$ is independent of ℓS^t for fixed B and ℓ , the second term $H(S_I | BLS^t, L = \ell)$ is also an integer multiple of $\ln q$. Therefore, if Eq. (6) holds for every B as verified in Eq. (11) and the RHS of Eq. (6) is $< \ln q$, then the LHS of Eq. (6) must be zero. Observe that under this assumption our modified construction is a universal k_{T+1}/m -strongly secure network coding in the exact sense of Definition 3. The parameter k_{T+1}/m is optimal according to [8].

E. Numerical example of explicit computation of required block size m

In this section we give a numerical example of computing required block length m in order to ensure the mutual information is below some value. In order to do so, we need an estimate of $\mathbf{E}[P_{S_I | S_I}(S_I^t | S_I^t)^\rho]$. We assume to have $\delta_{0.5} = 0.5$ in Eq. (12) at $\rho = 0.5$.

Let $q = 256$, $n = 10$, $\mu = 3$, $T = 5$, $k_i = 2m$ for all i . We do not have S_{T+1} . We want to ensure that we choose ℓ with probability at least $1 - 10^{-12}$ such that $I(S_i; BLS^t | L = \ell) < 10^{-6}$ for all $i = 1, \dots, 5$. By Eq. (11) we choose C_1 as

$$\begin{aligned} 2 \times nq^{\frac{(n+1)^2}{4}} (2^T - 1) / C_1 &= 10^{-12} \\ \Leftrightarrow C_1 &= 2 \times 10 \times 256^{11^2/4} (2^5 - 1) 10^{12} \end{aligned}$$

By using δ_ρ , we can upper bound the RHS of Eq. (6) as follows:

$$\begin{aligned} & C_1 q^{m\rho\mu} \mathbf{E}[P_{S_I | S_I}(S_I^t | S_I^t)^\rho] / \rho \\ &= C_1 \exp_q(m\rho(\mu + \frac{H_{1+\rho}(S_I^t | S_I^t)}{m \ln q})) / \rho \\ &\leq C_1 \exp_q(m\rho(\mu - n + k_I/m + \delta_\rho)) / \rho \quad (\text{by Eq. (12)}) \end{aligned} \quad (17)$$

In order to keep the above upper bound to be below 10^{-6} we have to choose

$$\begin{aligned} & C_1 \exp_q(m\rho(\mu - n + k_I/m + \delta_\rho)) / \rho < 10^{-6} \\ \Leftrightarrow m &> -\frac{\log_q(10^6 C_1 / \rho)}{\rho(\mu - n + k_I/m + \delta_\rho)} \\ \Leftrightarrow m &> -\frac{\log_{256}(10^6 \times 2 \times 10 \times 256^{121/4} (2^5 - 1) 10^{12} / 0.5)}{0.5(3 - 10 + 2 + 0.5)} \\ \Leftrightarrow m &\geq 17.3373 \end{aligned}$$

This means that we can choose $m = 18$ and should choose the matrix L at least as large as 180×180 over \mathbf{F}_{256} , which

is implementable. Recall that we assumed $n = 10$ outgoing (logical) links from the source node and that each outgoing link carries $m = 18$ symbols in single coding block in this example.

Remark 9: A vector in \mathbf{F}_q^{mn} can be identified with an element in $\mathbf{F}_{q^{mn}}$, and multiplication by a nonzero element in $\mathbf{F}_{q^{mn}}$ is an \mathbf{F}_q -linear mapping and can be identified with an element in \mathcal{L} . Let $\mathcal{L}_{\mathbf{F}_{q^{mn}}}$ be a commutative subgroup of \mathcal{L} whose elements can be identified with nonzero elements in $\mathbf{F}_{q^{mn}}$. By looking at the proof of Lemma 5 in Appendix B, we can see that $\mathcal{L}_{\mathbf{F}_{q^{mn}}}$ can be used in place of \mathcal{L} in our modified construction. Necessary storage space to record choice of an element in $\mathcal{L}_{\mathbf{F}_{q^{mn}}}$ is that of $mn \mathbf{F}_q$ symbols and is smaller than that of \mathcal{L} . Matrix multiplication by an element in $\mathcal{L}_{\mathbf{F}_{q^{mn}}}$ is at least as fast as that in \mathcal{L} .

IV. CONCLUSION

In the secure network coding, there was loss of information rate due to inclusion of random bits at the source node. Weakly and strongly secure network coding [3], [7], [22], [31] remove that loss of information rate by using multiple messages to be kept secret from an eavesdropper, which require huge computational complexity in code construction or huge finite field size. In addition to this, the previous studies assumed uniform and independent multiple messages, which seems too strong assumption in practice. In this paper, we have shown that random linear transform of multiple messages at the source node realizes the strongly secure network coding with arbitrary high probability with sufficiently large block length. We did not assume uniformity nor independence in multiple messages. Our numerical example in Section III-E showed that “sufficiently large block length” can be small.

APPENDIX A

PROOF OF PROPOSITION 4

In order to show Proposition 4, we introduce the following lemma.

Lemma 10: Under the same assumption as Proposition 4, we have

$$\mathbf{E}_f[\exp(-\rho H(F(A_1) | A_2, F = f))] \leq |\mathcal{A}_3|^{-\rho} + \mathbf{E}[P_{A_1 | A_2}(A_1 | A_2)^\rho] \quad (18)$$

for $0 \leq \rho \leq 1$.

Proof of Proposition 4:

$$\begin{aligned} & \mathbf{E}_f[\exp(\rho I(F(A_1); A_2 | F = f))] \\ &= \mathbf{E}_f[\exp(\rho H(F(A_1) | F = f) - \rho H(F(A_1), A_2 | F = f))] \\ &\leq \mathbf{E}_f[|\mathcal{A}_3|^\rho \exp(-\rho H(F(A_1), A_2 | F = f))] \\ &\leq |\mathcal{A}_3|^\rho (|\mathcal{A}_3|^{-\rho} + \mathbf{E}[P_{A_1 | A_2}(A_1 | A_2)^\rho]) \quad (\text{by Eq. (18)}) \\ &= 1 + |\mathcal{A}_3|^\rho \mathbf{E}[P_{A_1 | A_2}(A_1 | A_2)^\rho]. \end{aligned}$$

Proof of Lemma 10: Fix $a_2 \in \mathcal{A}_2$. The concavity of x^ρ for $0 \leq \rho \leq 1$ implies

$$\mathbf{E}_f\left[\sum_{a_3 \in \mathcal{A}_3} P_{f(A_1) | A_2}(a_3 | a_2)^{1+\rho}\right]$$

$$\begin{aligned}
&= \sum_{a_1 \in \mathcal{A}_1} P_{A_1|A_2}(a_1|a_2) \mathbf{E}_f \left[\sum_{a'_1 \in f^{-1}(f(a_1))} P_{A_1|A_2}(a'_1|a_2) \right]^\rho \\
&\leq \sum_{a_1 \in \mathcal{A}_1} P_{A_1|A_2}(a_1|a_2) \underbrace{\left(\mathbf{E}_f \left[\sum_{a'_1 \in f^{-1}(f(a_1))} P_{A_1|A_2}(a'_1|a_2) \right] \right)^\rho}_{(**)}. \quad (19)
\end{aligned}$$

For a fixed realization a_2 of A_2 , by the assumption in Proposition 4 two random variables F and A_1 are statistically independent, which implies the distribution of f in (**) is independent of a_1 . Since f is chosen from a family of two-universal hash functions defined in Definition 1, we have

$$\begin{aligned}
(**) &\leq P_{A_1|A_2}(a_1|a_2) + \sum_{a_1 \neq a'_1 \in \mathcal{A}_1} \frac{P_{A_1|A_2}(a'_1|a_2)}{|\mathcal{A}_3|} \\
&\leq P_{A_1|A_2}(a_1|a_2) + |\mathcal{A}_3|^{-1}.
\end{aligned}$$

Since any two positive numbers x and y satisfy $(x+y)^\rho \leq x^\rho + y^\rho$ for $0 \leq \rho \leq 1$, we have

$$(P_{A_1|A_2}(a_1|a_2) + |\mathcal{A}_3|^{-1})^\rho \leq P_{A_1|A_2}(a_1|a_2)^\rho + |\mathcal{A}_3|^{-\rho}. \quad (20)$$

By Eqs. (19) and (20) we can see

$$\mathbf{E}_f \left[\sum_{a_3 \in \mathcal{A}_3} P_{f(A_1)|A_2}(a_3|a_2)^{1+\rho} \right] \leq \sum_{a_1 \in \mathcal{A}_1} P_{A_1|A_2}(a_1|a_2)^{1+\rho} + |\mathcal{A}_3|^{-\rho}.$$

Taking the average over A_2 of the both sides of the last equation, we have

$$\mathbf{E}_f[\mathbf{E}_{A_1 A_2}[P_{f(A_1)|A_2}(f(A_1)|A_2)^\rho]] \leq \mathbf{E}_{A_1 A_2}[P_{A_1|A_2}(A_1|A_2)^\rho] + |\mathcal{A}_3|^{-\rho}. \quad (21)$$

Define $g(\rho) = \mathbf{E}_{A_1 A_2}[P_{f(A_1)|A_2}(f(A_1)|A_2)^\rho]$ as a function of ρ with fixed f and $P_{A_1|A_2}$, and $h(\rho) = \ln g(\rho)$. We have

$$\begin{aligned}
g'(\rho) &= \mathbf{E}_{A_1 A_2}[P_{f(A_1)|A_2}(f(A_1)|A_2)^\rho \ln P_{f(A_1)|A_2}(f(A_1)|A_2)], \\
g''(\rho) &= \mathbf{E}_{A_1 A_2}[P_{f(A_1)|A_2}(f(A_1)|A_2)^\rho (\ln P_{f(A_1)|A_2}(f(A_1)|A_2))^2], \\
h'(\rho) &= g'(\rho)/g(\rho), \\
h''(\rho) &= \frac{g''(\rho)g(\rho) - [g'(\rho)]^2}{g(\rho)^2}.
\end{aligned}$$

Define (A'_1, A'_2) to be the random variables that have the same joint distribution as (A_1, A_2) and statistically independent of A_1 and A_2 . To examine the sign of $h''(\rho)$ we compute

$$\begin{aligned}
&g''(\rho)g(\rho) - [g'(\rho)]^2 \\
&= \mathbf{E}_{A_1 A_2 A'_1 A'_2} [P_{f(A_1)|A_2}(f(A_1), A_2)^\rho P_{f(A_1)|A_2}(f(A'_1), A'_2)^\rho \\
&\quad \{(\ln P_{f(A_1)|A_2}(f(A_1)|A_2))^2 \\
&\quad - \ln P_{f(A_1)|A_2}(A_1|A_2) \ln P_{f(A_1)|A_2}(A'_1|A'_2)\}] \\
&= \frac{1}{2} \mathbf{E}_{A_1 A_2 A'_1 A'_2} [P_{f(A_1)|A_2}(f(A_1), A_2)^\rho P_{f(A_1)|A_2}(f(A'_1), A'_2)^\rho \\
&\quad \{(\ln P_{f(A_1)|A_2}(f(A_1)|A_2))^2 + (\ln P_{f(A_1)|A_2}(f(A'_1)|A'_2))^2 \\
&\quad - 2 \ln P_{f(A_1)|A_2}(f(A_1)|A_2) \ln P_{f(A_1)|A_2}(f(A'_1)|A'_2)\}] \\
&= \frac{1}{2} \mathbf{E}_{A_1 A_2 A'_1 A'_2} [P_{f(A_1)|A_2}(f(A_1), A_2)^\rho P_{f(A_1)|A_2}(f(A'_1), A'_2)^\rho \\
&\quad \{\ln P_{f(A_1)|A_2}(f(A_1)|A_2) - \ln P_{f(A_1)|A_2}(f(A'_1)|A'_2)\}^2] \\
&\geq 0.
\end{aligned}$$

This means that $h''(\rho) \geq 0$ and $h(\rho)$ is convex. We can see

$$\mathbf{E}_{A_1 A_2}[P_{f(A_1)|A_2}(f(A_1)|A_2)^\rho] = \exp(h(\rho))$$

$$\begin{aligned}
&\geq \exp(\underbrace{h(0)}_{=0} + \rho h'(0)) \\
&= \exp(-\rho H(f(A_1)|A_2)). \quad (22)
\end{aligned}$$

By Eqs. (21) and (22) we see that Eq. (18) holds. ■

APPENDIX B PROOF OF LEMMA 5

We shall prove Lemma 5 in this Appendix. Let \mathcal{L} be a subgroup of the group of all bijective linear maps on \mathbf{F}_q^{mn} . For $\vec{x} \in \mathbf{F}_q^{mn}$, the orbit $O(\vec{x})$ of \vec{x} under the action of \mathcal{L} is defined by

$$O(\vec{x}) = \{L\vec{x} \mid L \in \mathcal{L}\}.$$

Lemma 11: Let \vec{x}, \vec{y} be two different vectors belonging to $O(\vec{z})$. We have

$$|\{L \in \mathcal{L} \mid L\vec{z} = \vec{x}\}| = |\{L \in \mathcal{L} \mid L\vec{z} = \vec{y}\}|.$$

Proof: Let $K \in \mathcal{L}$ such that $K\vec{x} = \vec{y}$. We have

$$\begin{aligned}
&|\{L \in \mathcal{L} \mid L\vec{z} = \vec{x}\}| \\
&= |\{L \in \mathcal{L} \mid KL\vec{z} = K\vec{x}\}| \\
&= |\{L \in \mathcal{L} \mid KL\vec{z} = \vec{y}\}| \\
&= |\{L \in \mathcal{L} \mid L\vec{z} = \vec{y}\}|.
\end{aligned}$$

Lemma 12: Let B be an $m\mu \times mn$ matrix, $\ker(B) = \{\vec{x} \in \mathbf{F}_q^{mn} \mid B\vec{x} = \vec{0}\}$, and $\text{im}(B) = \{B\vec{x} \mid \vec{x} \in \mathbf{F}_q^{mn}\}$. The family of functions $\{BL \mid L \in \mathcal{L}\}$ with uniformly distributed L is a family of two-universal hash functions from \mathbf{F}_q^{mn} to $\text{im}(B)$ if and only if

$$\frac{|O(\vec{v}) \cap \ker(B)|}{|O(\vec{v})|} \leq \frac{1}{|\text{im}(B)|}$$

for all $\vec{v} \in \mathbf{F}_q^{mn} \setminus \{\vec{0}\}$.

Proof: With the uniform distribution on \mathcal{L} , LHS of Eq. (1) is equal to

$$\begin{aligned}
&\frac{|\{L \in \mathcal{L} \mid BL\vec{x}_1 = BL\vec{x}_2\}|}{|\mathcal{L}|} \\
&= \frac{|\{L \in \mathcal{L} \mid BL(\vec{x}_1 - \vec{x}_2) = \vec{0}\}|}{|\mathcal{L}|} \\
&= \frac{|\{L \in \mathcal{L} \mid L(\vec{x}_1 - \vec{x}_2) \in \ker(B)\}|}{|\mathcal{L}|} \\
&= \frac{|\{L \in \mathcal{L} \mid L(\vec{x}_1 - \vec{x}_2) \in O(\vec{x}_1 - \vec{x}_2) \cap \ker(B)\}|}{|\{L \in \mathcal{L} \mid L(\vec{x}_1 - \vec{x}_2) \in O(\vec{x}_1 - \vec{x}_2)\}|} \\
&= \frac{|O(\vec{x}_1 - \vec{x}_2) \cap \ker(B)|}{|O(\vec{x}_1 - \vec{x}_2)|} \text{ (by Lemma 11).}
\end{aligned}$$

Renaming $\vec{x}_1 - \vec{x}_2$ to \vec{v} proves the lemma. ■

Proposition 13: If \mathcal{L} is the set of all bijective linear maps on \mathbf{F}_q^{mn} , then $\{BL \mid L \in \mathcal{L}\}$ with uniformly distributed L is a family of two-universal hash functions from \mathbf{F}_q^{mn} to $\text{im}(B)$.

Proof: For a nonzero $\vec{v} \in \mathbf{F}_q^{mn}$, we have $O(\vec{v}) = \mathbf{F}_q^{mn} \setminus \{\vec{0}\}$, which implies

$$|O(\vec{v})| = |\mathbf{F}_q^{mn}| - 1,$$

$$|O(\vec{v}) \cap \ker(B)| = \frac{|\mathbf{F}_q^{mn}|}{|\text{im}(B)|} - 1.$$

By Lemma 12 we can see that the proposition is true. ■

Proof of Lemma 5: Lemma 5 is equivalent to Proposition 13. ■

ACKNOWLEDGMENT

The authors thank anonymous reviewers of NetCod 2011 and anonymous reviewers in the previous submission to this journal for carefully reading the previous manuscripts and pointing out its shortcomings. The first author would like to thank Prof. H. Yamamoto to teach him the secure multiplex coding, Dr. S. Watanabe to point out the relation between the proposed scheme and [22], J. Kurihara to point out the relation between the proposed scheme and [31], Dr. J. Muramatsu and Prof. T. Ogawa for the helpful discussion on the universal coding. A part of this research was done during the first author's stay at the Institute of Network Coding, the Chinese University of Hong Kong, and Department of Mathematical Sciences, Aalborg University. He greatly appreciates the hospitality by Prof. R. Yeung and Prof. O. Geil.

REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1206, Jul. 2000.
- [2] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
- [3] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proc. NetCod 2005*, Riva del Garda, Italy, Apr. 2005.
- [4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. 1979 of the National Computer Conference 48*, New York, USA, July 1979, pp. 313–317.
- [5] G. R. Blakley, and C. Meadows, "Security of ramp schemes," in *Advances in Cryptology – CRYPTO'84*, ed. G. R. Blakley and D. Chaum, Lecture Notes in Computer Science, vol. 196, pp. 242–268, Springer-Verlag, 1985.
- [6] M. Bloch and J. Barros, *Physical Layer Security*. Cambridge University Press, 2011.
- [7] N. Cai, "Valuable messages and random outputs of channels in linear network coding," in *Proc. IEEE ISIT 2009*, Seoul, Korea, Jun. 2009, pp. 413–417.
- [8] N. Cai and T. Chan, "Theory of secure network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 421–437, Mar. 2011.
- [9] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. 2002 IEEE ISIT*, Lausanne, Switzerland, Jul. 2002, p. 323. [Online]. Available: <http://iest2.ie.cuhk.edu.hk/~whyung/publications/secure.pdf>
- [10] —, "Network error correction, part II: Lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 37–54, 2006.
- [11] —, "A security condition for multi-source linear network coding," in *Proc. 2007 IEEE ISIT*, Nice, France, Jun. 2007, pp. 561–565.
- [12] —, "Secure network coding on a wiretap network," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.
- [13] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. System Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.
- [14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley Interscience, 2006.
- [15] S. El Rouayheb and E. Soljanin, "On wiretap networks II," in *Proc. ISIT 2007*, Nice, France, Jun. 2007, pp. 551–555.
- [16] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," to appear in *IEEE Trans. Inform. Theory*, arXiv:0907.3493.
- [17] H. Exton, *q-Hypergeometric Functions and Applications*, Halsted Press, 1983.
- [18] C. Fragouli, J.-Y. Le Boudec, and J. Widmer, "Network coding: An instant primer," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 1, pp. 63–68, Jan. 2006.
- [19] C. Fragouli and E. Soljanin, *Network Coding Applications*. NOW Publishers, 2007.
- [20] —, *Network Coding Fundamentals*. NOW Publishers, 2007.
- [21] L. Golshani, E. Pasha, and G. Yari, "Some properties of Rényi entropy and Rényi entropy rate," *Information Sciences*, vol. 179, no. 14, pp. 2426–2433, Jun. 2009.
- [22] K. Harada and H. Yamamoto, "Strongly secure linear network coding," *IEICE Trans. Fundamentals*, vol. E91-A, no. 10, pp. 2720–2728, Oct. 2008.
- [23] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inform. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.
- [24] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
- [25] D. Kobayashi, H. Yamamoto, and T. Ogawa, "How to attain the ordinary channel capacity securely in wiretap channels," in *Proc. 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Oct. 2005, pp. 13–18, arXiv:cs/0509047.
- [26] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. on Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
- [27] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
- [28] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Hanover, MA, USA: NOW Publishers, 2009.
- [29] R. Matsumoto and M. Hayashi, "Secure multiplex coding with a common message," in *Proc. 2011 IEEE ISIT*, Saint-Petersburg, Russia, Jul. 2011, pp. 1931–1935, arXiv:1101.4036.
- [30] —, "Secure multiplex network coding," in *Proc. IEEE NetCod 2011*, Beijing, China, Jul. 2011, arXiv:1102.3002.
- [31] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," in *Proc. ITW 2009*, Volos, Greece, Jun. 2009, pp. 281–285.
- [32] —, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.
- [33] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [34] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [35] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," *Electronics and Communications in Japan (Part I: Communications)*, vol. 69, no. 9, pp. 46–54, 1986, doi: 10.1002/ecja.4410690906.
- [36] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19–36, 2006.
- [37] Z. Zhang and R. W. Yeung, "A general security condition for multi-source linear network coding," in *Proc. 2009 IEEE ISIT*, Seoul, Korea, Jun. 2009, pp. 1155–1158.